The Hack Pack

Instruction Booklet

8 Pine Dale, Rainford ,Merseyside, WA11 8DP

The Hack Pack

Tape contents:

1)	Screen monitor	LOAD ""
2)	Memory monitor	CLEAR 32767: LOAD "" CODE: PRINT USR 32768
3)	AlkCode	CLEAR 28671: LOAD "" CODE: PRINT USR 28672
4)	SpeedCode	CLEAR 49999: LOAD "" CODE: PRINT USR 50000
5)	FireCode	CLEAR 25855: LOAD "" CODE: PRINT USR 25856
6)	Headerless file	- For use with 3,4,5.

Memory Monitor (2nd on tape)

The program will load and display ROM in the bottom left hand corner of the screen. This signifies that the program is now under your control. Press BREAK/SPACE to enter the program.

All inputs to and from the program will be in HEX (see conversion table in appendix) A complete list of the commands available now follow:-

(Q) List ASCII

Enter a number from 0000 to FFFF. The program will list the address you selected say, 7F12, as 7F12 33 3, with a cursor alongside. The first value is the memory location, the second is the value it contains and the third is the ascii value of it. Typing in a number or letter on the keyboard will insert the value of that character into the memory location.

Pressing ENTER will move you to the next memory location, whilst CAPS SHIFT will abort this mode.

For example if you have just loaded a basic program then enter the address 566B. This will list the basic and ignore hidden program lines, so you will see the basic as it really is. Typing other addresses will simply show the text from those addresses onwards.

(W) Ram page (128k machines only)

This will page in the memory banks which occupy the locations from C000 to FFFF . Insert a number from 0 to 7 for the bank required.

(R) Register dump

Lists the values of the spectrums internal registers and the values they had when the monitor was entered.

(Y) Return to BASIC

This option can be useful for taking anti-merge out of a program ie a program that crashes when you try MERGE "". Just load it in via option (L) and when it has finished loading use this option to return to basic, and you will break into it.

(P) HEX dump.

Type in an address and a window of 8 characters across by 16 down is displayed. This is handy for fast memory display.

(A) Block move.

A block mover for code, simply type in where from - to end of - and where you want it to go and it will do the rest.

(F) Find bytes. (Infinite life finder!)

Type in a start and end address of some code eg 5B00 and press ENTER. Then type the string of bytes that you wish to find eg 3E 05 32 for 5 lives in a game. It will then list all the locations that contain this string and will disassemble the surrounding code.

(J) Jump to.

Type in an address that you wish the program to jump to in memory. This will cause the program to exit the monitor and jump to the address specified executing the code at that address.

For example address 0000 would activate a reset.

(L) Load program.

This has two basic modes of use, which may seem strange at first!

If the program you wish to hack has a header then just type (L) and then ENTER to load it. Values obtained from the header will be remembered by the monitor eg the start address of the following code to be loaded. Programs will be loaded to the address specified in the header.

If the program does not have a header then you will have to tell the monitor where to place the program in memory. An example being C000 4000 and then ENTER.

(S) Save program.

This works on the same principal as the (L) command. If a file has been loaded in with a header, then pressing (S) and ENTER will save that file out with the same start address and length of bytes (still remembered from loading) complete with its header and any alterations that you have made.

But if you wanted to save your own program out then type in your own start address and length.

eg. (S) and 4000 1B00 would save out a headerless file from address 4000 of length 1B00 bytes.

(Z) Disassemble memory.

Type in an address and the program will disassemble the memory from that location ie converting bytes into op-codes. A time ago there were a lot of extra opcodes discovered and protection systems went mad using them. This will handle ALL the illegal opcodes and quite a few more!

(X) Exit a mode

Entering this in any mode quits the current mode of use.

Advanced Memory Monitor usage.

Nearly all Spectrum protection systems use some sort of encryption, this is usually an XOR of the spectrum code (a code up) or more commonly now the refresh register. This is the counter held in the cpu which counts every instruction the computer performs. Every spectrum monitor finds it impossible to single step any program containing the instructions LD A,R , LD R,A. This is the point when our ordinary hacker must give up because he knows that from now on every instruction is timed. However our monitor is able to give the cpu the times that it expects to see. Therefore you can single step through any type of protection and if you wish automatically decrypt it.

It is suggested that you read this section carefully, twice if possible and then attempt to use these functions.

(T) Trace mode.

This option gives you full control of any Z 80 program and it is here where the hack pack comes into its own. It can single step, decrypt loaders, in fact there is not much it cannot achieve if used correctly.

Typing (T) and then ENTER will take you into trace mode and will display the current contents of the program counter location.

By typing (T) and an address eg FE00, would display from address FE00 onwards and all operations continuing from this address onwards.

We will consider 2 example protection systems:

Speedlock
Players

Speedlock Hack

Yes, lets rip apart a speedlock. You can generally notice such a system on a program, they have a large basic header, border stripes, a screen$ which suddenly appears and a counter which ticks away in a corner in mins-secs-tenths of secs.

Load the speedlock program in on (L) mode. The speedlock RANDOMIZE USR in hex is 5D06 so we will use mode (T) with this address.

At the top of the screen you will see the instruction DI. Press ENTER about 12 times, during this the screen will go blank. Do no worry simply press (X) then press (T) ENTER and the screen will go back to normal. What you have done is moved part of speedlocks program, now type (B) FC00 then ENTER. The monitor will decrypt all of the program.

Be warned it takes a very, very long time. The program will stop when it reaches FC00 in memory.

(S) Set Program counter to..

This is handy for skipping code when tracing that you do not want to trace eg.

```
C000      DI
C001      PUSH AF
C002      PUSH BC
C003      LD BC,65535
C006      DEC BC                A long loop that we are
C007      LD A,B                not interested in tracing.
C008      OR C
C009      DJ NZ,C006
C00A      EI
```

By typing (S) and then address C00A we could miss out this time consuming piece of code.

(M) Display Memory PEEK contents

Displays the PEEK contents of the address that you specify onwards. Pressing ENTER continues the mode and (X) quits.

(6) Cursor up

(7) Cursor down

(1) Edit register under cursor

These keys allow you to alter the spectrums internal registers to the values that you want them to be. During the course of machine code or computer use the contents of these registers will alter. Using the above keys you can alter the contents. At the end of the instructions is a diagram of a typical program in trace mode with an explanation of the registers.

Players Hack

Now we can try a Players protection system with the monitor.

Players programs usually load in blue/black, having a small piece of BASIC at the beginning followed by a small block of code. It is this code that we are interested in so after loading this using option (L)

it will display something like ,

```
FRED    FE00 0120
```

Use option (Z) to disassemble the code from address FE00. You would see something like this :-

```
     FE00      DI
     FE01      LD HL,FF00
     FE04      XOR A
     FE05      LD R,A                   ; Skateboard construction set
     FE07      LD A,R                   ; (Front cover YS August)
     FE09      XOR (HL)
     FE0A      LD (HL),A
     FE0B      INC HL
     FE0C      LD A,H
     FE0D      OR L
     FE0E      JP NZ,FE07
     FE11      JP FF00
```

Notice the jump at the end, this must be important as it is where the program is going to next after executing the previous instructions. Type (X) to exit the disassembly. Press (T) and FE00. A whole list of registers is displayed (these are not important now). Notice how the program disassembles the current instruction at the top of the screen. Press ENTER once and it moves up an instruction and updates the screen display to whatever action that instruction performed. Keep pressing ENTER and soon you will see JP NZ,????.

(Pressing ENTER continuously is rather boring so here are some other trace modes of use).

(D) Break point.

This allows the trace mode to run until it meets the address you specify. Exit trace mode with (x) and then press (D) and then enter an address eg FE11, this is the location that said JP FE00. The monitor will now have placed a call back to itself at this address. Now dissassemble FE00 onward and you will see that code has appeared at your address FE11.

By typing (J) FE00 and then ENTER the monitor will run the code until it meets the call back that you defined ie address FE11 here. Control will then be passed to the monitor.

This mode can therefore be used to run blocks or routines and then come back to the monitor when it has finished therefore saving a lot of time.

(R) Return on RET

Pressing (R) and then ENTER will make the program run on until it hits a RET instruction.

To explain every mode in mass detail would probably take up a book. We have tried to give you a broad idea of what is possible. If you get stuck then you can contact the program author. To do this first write to Sigmasoft at our address with your question and we will forward your query.

The screen monitor.

This is a self contained miracle program which protects itself against attempts to wipe it out. During use there will be corruption on the screen but do not worry. Only the bottom third of the screen is used for display.

(Q) List BASIC

Typing (Q) 0000 would list line 0 and (Q) 0001 will list line 1, followed by a LINE END message indicating the end of the basic line. The program will ignore any attempt to hide the lines and colour codes are even ignored.

(E) E-line

Will list the last command typed into a computer before a program was run eg LOAD "": RANDOMIZE USR x.

This can be used to gain auto-start for games.

(Y) Return to BASIC

This is the same as the memory monitors option and breaks into almost any program.

(P) Hex dump

Same as memory monitor. (See NB1)

(A) Block Move

Same as memory monitor.

(S) Save code

The difference here is that this option will only save out a program with a header on. To save a headerless program use (K).

(J) Jump to

Same as memory monitor

(K) Save code

This is the headerless option and requires a start address and end address

(L) Load code

Same as memory monitor but only loads code with a header.

(C) Load headerless code

Same as (L) on memory monitor for loading headerless code and thus will require a start and end address.

(Z) Dissassemble

Same as memory monitor (see NB1)

(U) Header details

Displays the information from a loaded header onto the screen.

(M) Alter bytes

NB1

When using (P) or (Z) by pressing SYM SHIFT & V will direct output to a printer. Pressing N cancels this and displays information to the screen.

NB2

When using (H) and (Z) you can also specify a second address to stop at.

NB3

When using (L) and (K) in the screen monitor do not worry if your headers say that they start at 4000 hex or less or if your headerless block starts low down. The monitor ignores code loaded to less than 5B00.

NB4

Data is always loaded to its correct address. Memory monitor does not have this feature built in so large blocks of code (>8000 hex) may crash it.

ALKCODE, FIRECODE, SPEEDCODE are programs which load in a program protected by the relevant protection system. After choosing such a program by loading as detailed on page 1 then load the game you want to hack (that has that protection) into the spectrum. Once loaded the border will flash blue/red. Now load in the headerless file from tape and you will enter the monitor with full control of the game code.

Trace Mode Layout

```
STEP                                (1)

15ED RET                            (2)

IR   3F00                           (3)

          SZ H PNC                  (4)  STACK
AF'  00   01010101                  (5)  1E29
BC'  0002                           (6)  8102
DE'  0003                           (7)  5C3A
HL'  0004                           (8)  0101
                                        *1090

          SZ H PNC                  (9)
AF   00   10000111                  (A)
BC   0006                           (B)  (BC) 01 02 03 04 05
DE   0007                           (C)  (DE) 09 AF DE C9 20
HL   0008                           (D)  (HL) 21 34 56 29 C2

IX   0009                           (E)
IY   000A                           (F)
SP   0000                           (G)
PC   15ED                           (H)

M 8000 00 00 00 00 00 00            (I)
```

Explanation of diagram

```
1    Tells you what mode you are in eg SKIP/STEP etc
2    The program counter and whats in that location
3    |
4    |
5    |
6    |
7    |
8    The spectrums alternate registers and the values they hold
9    The spectrum flags (1=set) (0=unset)
A    |
B    |
C    |
D    |
E    |
F    |
G    |
H    The spectrums registers and the values they hold
I    What the (M) mode is currently pointing to
```

STACK : The contents of the spectrum stack ie pushed values. The (*) represents the value currently being used.

(HL) (DE) (BC) give the contents of the address pointed to by the register.

Appendix

Decimal-hexadecimal conversion table

Decimal 0–255 Hexadecimal 00–FF, Low byte

Dec.	Hex.	Dec.	Hex.	Dec.	Hex.	2's C.	Dec.	Hex.	2's C.
0	00	64	40	128	80	−128	192	C0	−64
1	01	65	41	129	81	−127	193	C1	−63
2	02	66	42	130	82	−126	194	C2	−62
3	03	67	43	131	83	−125	195	C3	−61
4	04	68	44	132	84	−124	196	C4	−60
5	05	69	45	133	85	−123	197	C5	−59
6	06	70	46	134	86	−122	198	C6	−58
7	07	71	47	135	87	−121	199	C7	−57
8	08	72	48	136	88	−120	200	C8	−56
9	09	73	49	137	89	−119	201	C9	−55
10	0A	74	4A	138	8A	−118	202	CA	−54
11	0B	75	4B	139	8B	−117	203	CB	−53
12	0C	76	4C	140	8C	−116	204	CC	−52
13	0D	77	4D	141	8D	−115	205	CD	−51
14	0E	78	4E	142	8E	−114	206	CE	−50
15	0F	79	4F	143	8F	−113	207	CF	−49
16	10	80	50	144	90	−112	208	D0	−48
17	11	81	51	145	91	−111	209	D1	−47
18	12	82	52	146	92	−110	210	D2	−46
19	13	83	53	147	93	−109	211	D3	−45
20	14	84	54	148	94	−108	212	D4	−44
21	15	85	55	149	95	−107	213	D5	−43
22	16	86	56	150	96	−106	214	D6	−42
23	17	87	57	151	97	−105	215	D7	−41
24	18	88	58	152	98	−104	216	D8	−40
25	19	89	59	153	99	−103	217	D9	−39
26	1A	90	5A	154	9A	−102	218	DA	−38
27	1B	91	5B	155	9B	−101	219	DB	−37
28	1C	92	5C	156	9C	−100	220	DC	−36
29	1D	93	5D	157	9D	−99	221	DD	−35
30	1E	94	5E	158	9E	−98	222	DE	−34
31	1F	95	5F	159	9F	−97	223	DF	−33
32	20	96	60	160	A0	−96	224	E0	−32
33	21	97	61	161	A1	−95	225	E1	−31
34	22	98	62	162	A2	−94	226	E2	−30
35	23	99	63	163	A3	−93	227	E3	−29
36	24	100	64	164	A4	−92	228	E4	−28
37	25	101	65	165	A5	−91	229	E5	−27
38	26	102	66	166	A6	−90	230	E6	−26
39	27	103	67	167	A7	−89	231	E7	−25
40	28	104	68	168	A8	−88	232	E8	−24
41	29	105	69	169	A9	−87	233	E9	−23
42	2A	106	6A	170	AA	−86	234	EA	−22
43	2B	107	6B	171	AB	−85	235	EB	−21
44	2C	108	6C	172	AC	−84	236	EC	−20
45	2D	109	6D	173	AD	−83	237	ED	−19
46	2E	110	6E	174	AE	−82	238	EE	−18
47	2F	111	6F	175	AF	−81	239	EF	−17
48	30	112	70	176	B0	−80	240	F0	−16
49	31	113	71	177	B1	−79	241	F1	−15
50	32	114	72	178	B2	−78	242	F2	−14
51	33	115	73	179	B3	−77	243	F3	−13
52	34	116	74	180	B4	−76	244	F4	−12
53	35	117	75	181	B5	−75	245	F5	−11
54	36	118	76	182	B6	−74	246	F6	−10
55	37	119	77	183	B7	−73	247	F7	−9
56	38	120	78	184	B8	−72	248	F8	−8
57	39	121	79	185	B9	−71	249	F9	−7
58	3A	122	7A	186	BA	−70	250	FA	−6
59	3B	123	7B	187	BB	−69	251	FB	−5
60	3C	124	7C	188	BC	−68	252	FC	−4
61	3D	125	7D	189	BD	−67	253	FD	−3
62	3E	126	7E	190	BE	−66	254	FE	−2
63	3F	127	7F	191	BF	−65	255	FF	−1

Decimal 0–65 280 Hexadecimal 00–FF, high byte

Decimal	Hex.	Decimal	Hex.	Decimal	Hex.	Decimal	Hex.
0	00	16 384	40	32 768	80	49 152	C0
256	01	16 640	41	33 024	81	49 408	C1
512	02	16 896	42	33 280	82	49 664	C2
768	03	17 152	43	33 536	83	49 920	C3
1 024	04	17 408	44	33 792	84	50 176	C4
1 280	05	17 664	45	34 048	85	50 432	C5
1 536	06	17 920	46	34 304	86	50 688	C6
1 792	07	18 176	47	34 560	87	50 944	C7
2 048	08	18 432	48	34 816	88	51 200	C8
2 304	09	18 688	49	35 072	89	51 456	C9
2 560	0A	18 944	4A	35 328	8A	51 712	CA
2 816	0B	19 200	4B	35 584	8B	51 968	CB
3 072	0C	19 456	4C	35 840	8C	52 224	CC
3 328	0D	19 712	4D	36 096	8D	52 480	CD
3 584	0E	19 968	4E	36 352	8E	52 736	CE
3 840	0F	20 224	4F	36 608	8F	52 992	CF
4 096	10	20 480	50	36 864	90	53 248	D0
4 352	11	20 736	51	37 120	91	53 504	D1
4 608	12	20 992	52	37 376	92	53 760	D2
4 864	13	21 248	53	37 632	93	54 016	D3
5 120	14	21 504	54	37 888	94	54 272	D4
5 376	15	21 760	55	38 144	95	54 528	D5
5 632	16	22 016	56	38 400	96	54 784	D6
5 888	17	22 272	57	38 656	97	55 040	D7
6 144	18	22 528	58	38 912	98	55 296	D8
6 400	19	22 784	59	39 168	99	55 552	D9
6 656	1A	23 040	5A	39 424	9A	55 808	DA
6 912	1B	23 296	5B	39 680	9B	56 064	DB
7 168	1C	23 552	5C	39 936	9C	56 320	DC
7 424	1D	23 808	5D	40 192	9D	56 576	DD
7 680	1E	24 064	5E	40 448	9E	56 832	DE
7 936	1F	24 320	5F	40 704	9F	57 088	DF
8 192	20	24 576	60	40 960	A0	57 344	E0
8 448	21	24 832	61	41 216	A1	57 600	E1
8 704	22	25 088	62	41 472	A2	57 856	E2
8 960	23	25 344	63	41 728	A3	58 112	E3
9 216	24	25 600	64	41 984	A4	58 368	E4
9 472	25	25 856	65	42 240	A5	58 624	E5
9 728	26	26 112	66	42 496	A6	58 880	E6
9 984	27	26 368	67	42 752	A7	59 136	E7
10 240	28	26 624	68	43 008	A8	59 392	E8
10 496	29	26 880	69	43 264	A9	59 648	E9
10 752	2A	27 136	6A	43 520	AA	59 904	EA
11 008	2B	27 392	6B	43 776	AB	60 160	EB
11 264	2C	27 648	6C	44 032	AC	60 416	EC
11 520	2D	27 904	6D	44 288	AD	60 672	ED
11 776	2E	28 160	6E	44 544	AE	60 928	EE
12 032	2F	28 416	6F	44 800	AF	61 184	EF
12 288	30	28 672	70	45 056	B0	61 440	F0
12 544	31	28 928	71	45 312	B1	61 696	F1
12 800	32	29 184	72	45 568	B2	61 952	F2
13 056	33	29 440	73	45 824	B3	62 208	F3
13 312	34	29 696	74	46 080	B4	62 464	F4
13 568	35	29 952	75	46 336	B5	62 720	F5
13 824	36	30 208	76	46 592	B6	62 976	F6
14 080	37	30 464	77	46 848	B7	63 232	F7
14 336	38	30 720	78	47 104	B8	63 488	F8
14 592	39	30 976	79	47 360	B9	63 744	F9
14 848	3A	31 232	7A	47 616	BA	64 000	FA
15 104	3B	31 488	7B	47 872	BB	64 256	FB
15 360	3C	31 744	7C	48 128	BC	64 512	FC
15 616	3D	32 000	7D	48 384	BD	64 768	FD
15 872	3E	32 256	7E	48 640	BE	65 024	FE
16 128	3F	32 512	7F	48 896	BF	65 280	FF